Statement of Work (SOW)
Defense Manpower Data Center
ORACLE Cloud Computing Services

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) located in Seaside, California has evolved into a world leader in Department of Defense (DoD) identity management, serving uniformed service members and their families across the globe. DMDC is the leader in joint information sharing and support on DoD human resource issues; the central source for identifying, authenticating, authorizing, and providing information on personnel during and after their affiliation with DoD; and the one, central access point for information and assistance on DoD entitlements, benefits, and medical readiness for uniformed service members, veterans, and their families.

2.0 BACKGROUND

DMDC is the DoD enterprise-wide provider of Humans Resource IT services and products leveraging extensive human resource focused data assets. DMDC operates the Defense Civilian Personnel Data System (DCPDS), a multifunction, web-based civilian HR information management and transaction processing system that supports approximately 900,000 civilian employee records (appropriated fund, non- appropriated fund, National Guard, and local nationals). Deployment of DCPDS began in October 1999, reaching Full Operating Capability (FOC) in September 2002. DCPDS is a global system supporting users in Asia, the Pacific, Europe and North America on a 24-hour, 7-days-a- week, basis. While DCPDS used a Commercial Off-The-Shelf (COTS) product (Oracle Enterprise Business Suite (EBS)), the system was highly-customized for the Federal and Defense environments. With over 500,000 process rules and 1.75M pay and benefit algorithm combinations, DCPDS sustains a complex set of personnel data that interfaces with the DoD payroll system and maintains over 40 other interfaces to external systems and databases. This complexity and number of interfaces resulted in increased sustainment costs and drove the need for HR reforms within the DoD.

The Reform Management Group (RMG) is a Department of Defense (DoD) decision making body comprised of Senior DoD officials with the goal of improving and streamlining the Department's business processes in accordance with the priorities that Secretary Mattis delineated in the National Defense Strategy released January 19, 2018. On May 23, 2018, the RMG, led by the Deputy Secretary of Defense (DEPSECDEF), made the decision to enable the delivery of a modern capability. That decision led to the selection of an Oracle Software as a Service (SaaS) / Human Capital Management (HCM) Cloud Platform.

In order to comply with DoD Chief Information Officer (CIO) Directives, DMDC has established a Fit for Purpose Cloud and has started migration to cloud based services and requires continued use of Oracle Cloud Infrastructure (OCI) Infrastructure-as-a-Service (IaaS) in order to provide a highly-reliable, scalable and low-cost infrastructure platform in the cloud that offers DMDC users the ability to utilize, stand up and take down IT infrastructure (both programs and platforms) on demand. The on-demand nature of commercial cloud services reduces the necessity for DMDC users to expend the time and resources required to procure, sustain and maintain IT infrastructure which may only be needed for limited periods of time.

The Defense Civilian Human Resources Management System (DCHRMS) will replace the DCPDS, and move the Human Resources (HR) information system (HRIS) from six separate databases that maintain DoD employee records into one integrated enterprise database. DCHRMS is a Human Resource (HR) information system (HRIS) that will support civilian HR management, establish a single employee record, and create standardized personnel data across the enterprise. It is a cloud-based system that built on Oracle's Fusion HCM Base Cloud Software as a Service to provide a single civilian personnel service capability for the DoD.

DMDC has utilized OCI services for over a year. In that time, DMDC has migrated its Civilian Personnel IT Portfolio into OCI and is ready to expand the DMDC Fit for Purpose Cloud for additional DMDC portfolios by utilizing OCI services such as: compute, storage, databases, logging and monitoring, capacity management and provisioning, high-speed computing/analytics, virtual private cloud and web hosting to complete the transition out of the On-Premise data

centers into a Cloud environment per DoD guidance.

This requirement is a continuing effort to migrate DMDC applications from the data centers located in Seaside, CA and Columbus, OH to OCI in accordance with DoD CIO mandated Data Center Closure Guidance and includes cloud-based services to continue hosting the Department of Defense's (DoD) Civilian HR Information Technology (IT) portfolio, aligning with Federal and DoD initiatives, specifically the DoD CIO approved Business Case Analysis (BCA). Additionally, in order to prepare for the operational version of the DCHRMS program, the government must continue the subscription to Oracle Fusion of one license per user, a total of 900,000 Oracle Fusion licenses prior to full deployment.

The Oracle Cloud Service Offering will provide the next generation transactional Civilian HR system, DCHRMS, in a commercial-based HCM Solution along with the infrastructure for additional capabilities required to meet the DMDC mission. The Oracle HCM/Fusion Software licenses and technical support will replace the current Defense Civilian Personnel Data System (DCPDS) while the Oracle Cloud Infrastructure (OCI) will host the other existing applications.

3.0 SCOPE

This requirement focuses on the hosting of persistent Non-classified Internet Protocol (IP) Router Network (NIPRNet) systems currently hosted at the DMDC enclave at the Columbus, OH Defense Enterprise Computing Center (DECC) and the Seaside, CA Defense Manpower Data Center; continued hosting of the DoD Civilian HR IT portfolio; Oracle HCM SaaS; software licenses; technical support and Oracle University instructor led training for use of the HCM Cloud as well as Reporting Analytics. The Contractor shall provide the materials and space necessary to accomplish Oracle Cloud Infrastructure-as-a-Service (IaaS) environment and support necessary for cloud services: compute, storage, databases, logging and monitoring, capacity management and provisioning, high-speed computing/analytics, virtual private cloud and web hosting per the standard Service Level Agreements (SLA). The Contractor must be an authorized brand reseller of Oracle at the Gold or Platinum Partner level and the Cloud Service Offering (CSO) must be certified at the DoD Cloud Computing Security Requirements Guide (SRG) Impact Level 4 (IL4) or above.

In addition to OCI IaaS for the Fit for Purpose Cloud, DMDC requires Oracle SaaS environment space; user licenses infrastructure, and technical support to continue to operate its Civilian Personnel IT Portfolio and its next generation transactional Human Resources (HR) System, the Defense Civilian Human Resources Management System (DCHRMS), in a commercial-based Human Capital Management (HCM) Solution. The DCHRMS system is required to be operational within the Oracle Fusion SaaS environment.

DMDC also requires Oracle Fusion Software and licenses including DCHRMS Performance and Goal Management licenses; and DCPDS EBS maintenance to continue the operation of the DCHRMS Human Capital Management (HCM) environment as well as space in the OCI Oracle IaaS environment with the technical services to assist DMDC to accomplish the migration of all remaining applications from the Seaside and Columbus Data Centers.

Lastly, DMDC requires Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions.

4.0 REQUIREMENTS *The Contractor shall*:

4.1 Infrastructure as a Service (IaaS): Provide IaaS within the Oracle Cloud Infrastructure (OCI) environment ~~.~~in accordance with the Bill of Materials. ~~-~~Performance includes at a minimum:

4.1.1 Provide Compute, Storage, Network, Database Backup, Disaster Recovery, and other capabilities in the environment.

4.1.2 Provide Oracle expertise in supporting the configuration and operations of the environment per the standard OEM SLA identified at https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html#paas-iaas. ~~If Oracle enhances the SLAs post award, such SLA shall apply to this order without additional cost to the Government.~~

4.1.3 Provide Oracle IaaS environment for Test, Development and Production.

4.1.4 Provide confirmation of, and maintain DoD Cloud Computing Security Requirements Guide (SRG) Impact Level (IL4) minimum certification.

4.1.5 DMDC retains ownership of any user created/loaded data and application(s) hosted on vendor's infrastructure, and maintains the right to request full copies of these at any time including access to and account information required to access all government data and government information.

4.2 Software as a Service (SaaS): Provide DMDC SaaS software licenses for Oracle Fusion to meet the needs of the DCHRMS program, in accordance with the Bill of Materials.

4.2.1 Renew non-production HCM Fusion environment for up to 5,000 users.

4.2.2 Within the existing Period of Performance, ~~Provide~~ provide the option to continue using Shelved On Premise Licenses and receiving the Limited On Premise Support for up to an additional six (6) consecutive month period by (1) sending written notice of such election at least thirty (30) days before the end of the Initial Transition Period, and (2) providing Limited On Premise Support for such period in three-month increments (each such three-month increment is called an "Extended Transition Period" and collectively, the "Extended Transition Periods"). For each Extended Transition Period, billing will be quarterly in arrears a net fee equal to eight percent (8%) of the annual support fee for the Shelved On Premise Licenses in the most recent annual support renewal order.

~~4.2.3 Provide~~Provide phased ability to load 900,000 total hosted employee records (but no more licenses than the government has purchased) for test purposes of the migration process prior to production implementation. Testing shall be in accordance with either (a) the already-granted Interim Authority to Test (IATT) if the cloud services being tested lack DOD SRG IL-4 or higher authorizations or (b) the relevant cloud services' DOD SRG IL-4 or higher authorizations." ~~phased ability to load 900,000 total hosted employee records (but no more licenses than the government has purchased) for test purposes of the migration process prior to production implementation. Testing shall be in accordance with granted Interim Authority to Test (IATT).~~

~~4.2.4~~4.2.3

4.3 Provide Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions

5.0 DELIVERABLES

Deliverable	PWS Ref.	Delivery Date
Oracle IaaS environment access for Test, Development and Production environments	4.1	Expedited, but no later than 15 days of Award
Fusion Human Capital Management Base Cloud Service (License numbers)	4.2	Expedited, but no later than 15 days of Award
All other IaaS, SaaS, as outlined in Appendices and optional CLINs	4.2	As indicated in in the Bill of Materials
Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions	4.3	Scheduling and coordination of requirements listed in the Bill of Materials to begin no later than 15 days of Award

6.0 CONTRACT ADMINISTRATION

6.1 Government Points of Contact

The identified individuals are responsible to oversee contract performance and the Contractor is responsible to coordinate with the identified individuals.

GSA Contracting Officer
Ms. Melissa DiTomaso
100 S. Independence Mall West
Philadelphia, PA 19106
Melissa.DiTomaso@gsa.gov
(215) 446-4892

GSA Contract Specialist
Mr. Katie Hughes
100 S. Independence Mall West
Philadelphia, PA 19106
katie.hughes@gsa.gov
(215)-446-4735

GSA Contracting Officer's Representative
Mr. Ruslan Gorbonos
100 S. Independence Mall West
Philadelphia, PA 19106
Ruslan.Gorbonos@gsa.gov
(215)-446-5820

DMDC COR: Will be notified Post Award

6.2 Post Award Conference

The Contractor shall participate in a Government-scheduled post-award orientation Task Order award or in accordance with Federal Acquisition Regulation Subpart 42.5. Within 7 work days of award the Contractor shall conduct an orientation briefing for the Government. The intent of the briefing is to initiate the communication process between the Government and Contractor by introducing key task participants and explaining their roles, reviewing communication ground rules, and assuring a common understanding of subtask requirements and objectives. The Orientation Briefing's place, date and time shall be mutually agreed upon by both parties within a week from the date of award. The completion of this briefing will result in the introduction of both Contractor and Government personnel performing work under this contract. The Contractor will demonstrate confirmation of their understanding of the work to be accomplished under this SOW.

6.3 Contract Type

This is a firm fixed price task order.

6.4 Period of Performance

The period of performance is one (1) ~~11~~10-month base period plus two (2) 12-month option periods.

Option periods will be exercised at the Government's unilateral right in accordance with FAR 52.217-9 - Option to Extend the Term of the Contract (Mar 2000). The government may extend the term of this contract by written notice to the contractor within thirty (30) calendar days before the contract expires; provided that the government gives the contractor a preliminary written notice of its intent to extend at least sixty (60) calendar days before the contract expires. The preliminary notice does not commit the government to an extension. If the government exercises an option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, shall not exceed ~~sixty~~ thirty-four (~~60~~34) months.

7.0 OTHER ADMINISTRATIVE REQUIREMENTS

7.1 Records and Data

The Government will be sole owner of all technical data, any user created/loaded data and application(s) hosted on vendor's infrastructure, and maintains the right to request full copies of these at any time including access to and account information required to access all government data and government ~~information.software developed, and infrastructure designed under this project. The~~information. The Contractor shall deliver to DMDC all software, software licenses, data, form, fit and data first produced (including source code), written documents and reports to include, at a minimum, system change plans, various operations procedures and planning documents, meeting minutes, reports, manuals, training text, program management reviews, financial status reports, and any other documents created in support of this agreement or task orders. All system documentation shall be updated to remain current with each software development activity/phase. Unless otherwise stated in the orders, the Contractor shall submit deliverables to the COR or his or her designee. The Government will include review times and response to review comments in the orders. The COR will serve as DMDC's focal point for accepting the deliverables unless an order provides for other procedures.

7.2 Limited Use of Data

Performance of this effort may require the Contractor to access and use data and information proprietary to a Government agency or Government Contractor which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others. Contractor and/or Contractor personnel shall not divulge or release data or information developed or obtained in performance of this effort, until made public by the Government, except to authorize Government personnel or upon written approval of the Contracting Officer (CO). The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort. Nothing herein shall preclude the use of any data independently acquired by the Contractor without such limitations or prohibit an agreement at no cost to the Government between the Contractor and the data owner which provides for greater rights to the Contractor.

7.3 Disclosure of Information

Information made available to the Contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way without the written agreement of the Contracting Officer. The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information. Each Contractor or employee of the Contractor to whom information may be made available or disclosed shall be notified in writing by the Contractor that such information may be disclosed only for a purpose and to the extent authorized herein.

7.4 Breach Response

DoD 5400.11-R, "DoD Privacy Program," May 14, 2007, defines a breach as the "actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected." The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The Contractor shall also comply with federal laws relating to freedom of information and records management. Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access, the contractor/subcontractor shall immediately and simultaneously notify the COR, the designated Cyber Security Officer, and Privacy Officer for the contract within one (1) hour. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to DMDC assets, or sensitive information, or an action that breaches DMDC security procedures.

The Contractor shall adhere to the reporting and response requirements set forth in the Office of the Secretary of Defense (OSD) Memorandum 1504-07, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," June 5, 2009; DoD 5400.11-R, and applicable DMDC Privacy Office guidance. The Contractor shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of Protected Information by the Contractor in violation of the

requirements of this Clause.
In the event of a data breach or privacy incident involving contractor processes under this contract, the Contractor shall be liable to DMDC for liquidated damages for a specified amount per affected individual to cover the cost of providing credit protection services to those individuals.

7.5 Invoicing

The following clauses are incorporated into the task or contract. A monthly status report shall accompany each invoice submitted in ITSS.

Clause #1 – Invoices

The Period of Performance (POP) for each invoice shall be for ~~one calendar month~~each quarter to align with Oracle's invoicing practices. ~~The contractor shall submit only one invoice per month per order/contract.~~ The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

1. The end of the invoiced month (for services) or
2. The end of the month in which the products (commodities) or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Cost Type, Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It shall also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, as well as the grand total of all costs incurred and invoiced.

For Cost Type, Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" for hours and dollars. Total average monthly "burn rate" may be provided in the Monthly Status Report that accompanies the invoice. The invoice shall also include running totals for both hours and dollars.

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Note: For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items:

Charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.
- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number, task item, and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration
P.O. Box 6200-29
Portland, OR 97228-6200

Posting Acceptance Documents: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS, to allow the client and GSA COTR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following option in accepting and certifying services:

a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Task Order Number
2. Task Order ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)
10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

Final Invoice: Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COTR before payment is processed, *if necessary.*

The Government reserves the right to modify invoicing requirements at its discretion. The Contractor shall comply with any revised invoicing requirements at no additional cost to the Government

Close-out Procedures
General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

7.6 Organizational Conflict of Interest

Contractor and subcontractor personnel performing work under this contract may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

7.7 Non-Disclosure Requirements

All contractor personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the contract issued which requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit a Contractor Non-Disclosure Agreement" Form. This is required prior to the commencement of any work on such task order and whenever replacement personnel are proposed under an ongoing task order. Any information obtained or provided in the performance of this contract is only to be used in the performance of the task order. The Contractor shall take the necessary steps in accordance with Government regulations to prevent disclosure of such information to any party outside the Government and to indoctrinate its personnel who have access to sensitive information and the relationship under which the Contractor has possession of or access to the information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information will be used for the profit of any party other than those furnishing the information. The Nondisclosure Agreement for Contractor Employees shall be signed by all indoctrinated personnel and forwarded to the Contracting Officer Representative (COR) for retention, prior to work commencing. The Contractor shall restrict access to sensitive/ proprietary information to the minimum number of employees necessary for contract/Task order performance.

7.8 Security Requirements: The Contractor shall:

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. This must include compliance with Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG), March 6, 2017 and NIST 800- 53v4.

For non-production environments, the parties agree that the Oracle Cloud Service NASA SEWP V Supplemental Terms and Conditions v033018 rev1 (STC), incorporated and attached hereto, including Oracle's Data Processing Agreement (DPA), and other service specifications (which define the administrative, physical, technical and other safeguards applied to the government's content residing in the services environment) satisfy the requirements of this section, excepting that to the extent that the STCs or DPA are precluded by Federal law (e.g., the Freedom of Information Act, the Federal Acquisition Regulation, Anti-deficiency Act, Contract Disputes Act), including and in addition to, among other things, where those documents apply foreign law (e.g., the European Union General Data Protection Regulation); permit data storage or processing outside of the United States; limit the Government's termination or dispute rights; require the Government to indemnify the Contractor or OEM; or permit the disclosure of the Government's Confidential Information; those provisions shall not apply.

Following notification by Oracle, the Contractor shall immediately communicate in writing (electronic correspondence acceptable) to the Government, any change to Oracle's FedRAMP moderate, DOD IL-4 certifications. This includes the addition or deletion of any service offerings or capabilities or changes to pricing structures.

The Contractor shall allow access only to those employees who need to perform work under this contract. The Contractor shall ensure that its employees will not discuss, divulge or disclose any information about government services to any person or entity except those persons within the Contractor's organization directly concerned with

the performance of the contract.

The Contractor is responsible for ensuring employees performing work under this contract have appropriate background checks and/or vetting completed and are trustworthy to perform services under this contract.

The contractor shall report Cybersecurity incidents pertaining to government services to the government ~~within one (1) hour of discovery.~~ Reporting will be done within 24 hours for root level intrusion and data compromise with subsequent reporting every 24 hours until the incident is closed. The Contractor shall also notify the COR and KO at the time the incident is reported.

The Contractor shall not use, distribute, disclose or modify government data.

8.0 CLAUSES

- GSA Invoicing Clause
- 52.203-13 Contractor Code of Business Ethics and Conduct (OCT 2015)
- 52.204-18 Commercial and Government Entity Code Maintenance (JUL 2016)
- 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)
- 52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Dec 2019)
- 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)
- 52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015)
- 52.212-4 Contract Terms and Conditions-Commercial Items (OCT 2018)
- 52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders-Commercial Items (MAR 2020)
- 52.217-7 Option for Increased Quantity-Separately Priced Line Item (Mar 1989)
- 52.217-8 Option to Extend Services (Nov 1999)
- 52.219-6 Notice Of Total Small Business Set-Aside (MAR 2020)
- 52.219-8 Utilization of Small Business Concerns (Oct 2018)
- 52.219-13 Notice of Set-Aside of Orders (Mar 2020)
- 52.219-14 Limitations on Subcontracting (Mar 2020)
- 52.219-28 Post-Award Small Business Program Rerepresentation (Mar 2020)
- ~~52.223-16 Acquisition of EPEAT®-Registered Personal Computer Products (Oct 2015)~~
- 52.224-1 Privacy Act Notification (Apr 1984)
- 52.224-2 Privacy Act (Apr 1984)
- 52.227-01 Authorization and Consent (Dec 2007)
- ~~52.227-03 Patent Indemnity (Apr 1984)~~
- ~~52.227-06 Royalty Information (Apr 1984)~~
- ~~52.227-09 Refund of Royalties (Apr 1984)~~
- 52.227-19 Commercial Computer Software License (Dec 2007)
- ~~52.225-5 Trade Agreements (Oct 2019)~~
- 52.232-39 Unenforceability of Unauthorized Obligations (Jun 2013)
- 52.232-40 Providing Accelerated Payments to Small Business Subcontractors (Dec 2013)
- 52.239-1 Privacy or Security Safeguards (Aug 1996)
- 252.201-7000 CONTRACTING OFFICER'S REPRESENTATIVE (DEC 1991)
- 252.203-7002 REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (SEP 2013)

- 252.203-7003 AGENCY OFFICE OF THE INSPECTOR GENERAL (AUG 2019)
- 252.203-7005 REPRESENTATION RELATING TO COMPENSATION OF FORMER DOD OFFICIALS (NOV 2011)
- 252.204-7000 DISCLOSURE OF INFORMATION (OCT 2016)
- ~~252.204-7002 PAYMENT FOR CONTRACT LINE OR SUBLINE ITEMS NOT SEPARATELY PRICED (APR 2020)~~
- 252.204-7003 CONTROL OF GOVERNMENT PERSONNEL WORK PRODUCT (APR 1992)
- ~~252.204-7004 LEVEL I ANTITERRORISM AWARENESS TRAINING FOR CONTRACTORS (FEB 2019)~~
- 252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (OCT 2016)
- 252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)
- 252.204-7016 COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES—REPRESENTATION (DEC 2019)
- 252.204-7017 PROHIBITION ON THE ACQUISITON OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES—REPRESENTATION (DEC 2019)
- 252.204-7018 PROHIBITION ON THE ACQUISITION OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES (DEC 2019)
- 252.205-7000 PROVISION OF INFORMATION TO COOPERATIVE AGREEMENT HOLDERS (DEC 1991)
- ~~252.211-7003 ITEM UNIQUE IDENTIFICATION AND VALUATION (MAR 2016)~~
- 252.215-7008 ONLY ONE OFFER (JUL 2019)
- 252.215-7013 SUPPLES AND SERVICES PROVIDED BY NONTRADITIONAL DEFENSE CONTRACTORS (JAN 2018)
- 252.227-7000 NON-ESTOPPEL (OCT 1966)
- ~~252.227-7015 TECHNICAL DATA—COMMERCIAL ITEMS (FEB 2014)~~
- ~~252.227-7025 LIMITATIONS ON THE USE OR DISCLOSURE OF GOVERNMENT-FURNISHED~~
- ~~252.227-7037 VALIDATION OF RESTRICTIVE MARKINGS ON TECHNICAL DATA (SEP 2016)~~
- 252.232-7007 LIMITATION OF GOVERNMENT S OBLIGATION (APR 2014)
- 252.232-7010 LEVIES ON CONTRACT PAYMENTS (DEC 2006)
- ~~252.239-7000 PROTECTION AGAINST COMPROMISING EMANATIONS (OCT 2019)~~
- ~~252.239-7001 INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION (JAN 2008)~~
- 252.239-7009 REPRESENTATION OF USE OF CLOUD COMPUTING (SEP 2015)
- 252.239-7010 CLOUD COMPUTING SERVICES (OCT 2016)
- 252.243-7001 PRICING OF CONTRACT MODIFICATIONS (DEC 1991)
- 252.243-7002 REQUESTS FOR EQUITABLE ADJUSTMENT (DEC 2012)
- 252.244-7000 SUBCONTRACTS FOR COMMERCIAL ITEMS AND COMMERCIAL COMPONENTS (DOD CONTRACTS) (JUN 2013)
- ~~252.246-7003 NOTIFICATION OF POTENTIAL SAFETY ISSUES (JUN 2013)~~
- ~~252.246-7005 NOTICE OF WARRANTY TRACKING OF SERIALIZED ITEMS (MAR 2016)~~
- ~~252.246-7006 WARRANTY TRACKING OF SERIALIZED ITEMS (MAR 2016)~~
- ~~252.247-7022 REPRESENTATION OF EXTENT OF TRANSPORTATION BY SEA (JUN 2019)~~
- ~~252.247-7023 TRANSPORTATION OF SUPPLIES BY SEA—BASIC (FEB 2019)~~
- 552.216-74 Task-Order and Delivery-Order Ombudsman (Jan2017)

Statement of Work (SOW)
Defense Manpower Data Center
ORACLE Cloud Computing Services

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) located in Seaside, California has evolved into a world leader in Department of Defense (DoD) identity management, serving uniformed service members and their families across the globe. DMDC is the leader in joint information sharing and support on DoD human resource issues; the central source for identifying, authenticating, authorizing, and providing information on personnel during and after their affiliation with DoD; and the one, central access point for information and assistance on DoD entitlements, benefits, and medical readiness for uniformed service members, veterans, and their families.

2.0 BACKGROUND

DMDC is the DoD enterprise-wide provider of Humans Resource IT services and products leveraging extensive human resource focused data assets. DMDC operates the Defense Civilian Personnel Data System (DCPDS), a multifunction, web-based civilian HR information management and transaction processing system that supports approximately 900,000 civilian employee records (appropriated fund, non- appropriated fund, National Guard, and local nationals). Deployment of DCPDS began in October 1999, reaching Full Operating Capability (FOC) in September 2002. DCPDS is a global system supporting users in Asia, the Pacific, Europe and North America on a 24-hour, 7-days-a- week, basis. While DCPDS used a Commercial Off-The-Shelf (COTS) product (Oracle Enterprise Business Suite (EBS)), the system was highly-customized for the Federal and Defense environments. With over 500,000 process rules and 1.75M pay and benefit algorithm combinations, DCPDS sustains a complex set of personnel data that interfaces with the DoD payroll system and maintains over 40 other interfaces to external systems and databases. This complexity and number of interfaces resulted in increased sustainment costs and drove the need for HR reforms within the DoD.

The Reform Management Group (RMG) is a Department of Defense (DoD) decision making body comprised of Senior DoD officials with the goal of improving and streamlining the Department's business processes in accordance with the priorities that Secretary Mattis delineated in the National Defense Strategy released January 19, 2018. On May 23, 2018, the RMG, led by the Deputy Secretary of Defense (DEPSECDEF), made the decision to enable the delivery of a modern capability. That decision led to the selection of an Oracle Software as a Service (SaaS) / Human Capital Management (HCM) Cloud Platform.

In order to comply with DoD Chief Information Officer (CIO) Directives, DMDC has established a Fit for Purpose Cloud and has started migration to cloud based services and requires continued use of Oracle Cloud Infrastructure (OCI) Infrastructure-as-a-Service (IaaS) in order to provide a highly-reliable, scalable and low-cost infrastructure platform in the cloud that offers DMDC users the ability to utilize, stand up and take down IT infrastructure (both programs and platforms) on demand. The on-demand nature of commercial cloud services reduces the necessity for DMDC users to expend the time and resources required to procure, sustain and maintain IT infrastructure which may only be needed for limited periods of time.

The Defense Civilian Human Resources Management System (DCHRMS) will replace the DCPDS, and move the Human Resources (HR) information system (HRIS) from six separate databases that maintain DoD employee records into one integrated enterprise database. DCHRMS is a Human Resource (HR) information system (HRIS) that will support civilian HR management, establish a single employee record, and create standardized personnel data across the enterprise. It is a cloud-based system that built on Oracle's Fusion HCM Base Cloud Software as a Service to provide a single civilian personnel service capability for the DoD.

DMDC has utilized OCI services for over a year. In that time, DMDC has migrated its Civilian Personnel IT Portfolio into OCI and is ready to expand the DMDC Fit for Purpose Cloud for additional DMDC portfolios by utilizing OCI services such as: compute, storage, databases, logging and monitoring, capacity management and provisioning, high-speed computing/analytics, virtual private cloud and web hosting to complete the transition out of the On-Premise data

centers into a Cloud environment per DoD guidance.

This requirement is a continuing effort to migrate DMDC applications from the data centers located in Seaside, CA and Columbus, OH to OCI in accordance with DoD CIO mandated Data Center Closure Guidance and includes cloud-based services to continue hosting the Department of Defense's (DoD) Civilian HR Information Technology (IT) portfolio, aligning with Federal and DoD initiatives, specifically the DoD CIO approved Business Case Analysis (BCA). Additionally, in order to prepare for the operational version of the DCHRMS program, the government must continue the subscription to Oracle Fusion of one license per user, a total of 900,000 Oracle Fusion licenses prior to full deployment.

The Oracle Cloud Service Offering will provide the next generation transactional Civilian HR system, DCHRMS, in a commercial-based HCM Solution along with the infrastructure for additional capabilities required to meet the DMDC mission. The Oracle HCM/Fusion Software licenses and technical support will replace the current Defense Civilian Personnel Data System (DCPDS) while the Oracle Cloud Infrastructure (OCI) will host the other existing applications.

3.0 SCOPE

This requirement focuses on the hosting of persistent Non-classified Internet Protocol (IP) Router Network (NIPRNet) systems currently hosted at the DMDC enclave at the Columbus, OH Defense Enterprise Computing Center (DECC) and the Seaside, CA Defense Manpower Data Center; continued hosting of the DoD Civilian HR IT portfolio; Oracle HCM SaaS; software licenses; technical support and Oracle University instructor led training for use of the HCM Cloud as well as Reporting Analytics. The Contractor shall provide the materials and space necessary to accomplish Oracle Cloud Infrastructure-as-a-Service (IaaS) environment and support necessary for cloud services: compute, storage, databases, logging and monitoring, capacity management and provisioning, high-speed computing/analytics, virtual private cloud and web hosting per the standard Service Level Agreements (SLA). The Contractor must be an authorized brand reseller of Oracle at the Gold or Platinum Partner level and the Cloud Service Offering (CSO) must be certified at the DoD Cloud Computing Security Requirements Guide (SRG) Impact Level 4 (IL4) or above.

In addition to OCI IaaS for the Fit for Purpose Cloud, DMDC requires Oracle SaaS environment space; user licenses infrastructure, and technical support to continue to operate its Civilian Personnel IT Portfolio and its next generation transactional Human Resources (HR) System, the Defense Civilian Human Resources Management System (DCHRMS), in a commercial-based Human Capital Management (HCM) Solution. The DCHRMS system is required to be operational within the Oracle Fusion SaaS environment.

DMDC also requires Oracle Fusion Software and licenses including DCHRMS Performance and Goal Management licenses; and DCPDS EBS maintenance to continue the operation of the DCHRMS Human Capital Management (HCM) environment as well as space in the OCI Oracle IaaS environment with the technical services to assist DMDC to accomplish the migration of all remaining applications from the Seaside and Columbus Data Centers.

Lastly, DMDC requires Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions.

4.0 REQUIREMENTS *The Contractor shall*:

4.1 Infrastructure as a Service (IaaS): Provide IaaS within the Oracle Cloud Infrastructure (OCI) environment in accordance with the Bill of Materials. Performance includes at a minimum:

4.1.1 Provide Compute, Storage, Network, Database Backup, Disaster Recovery, and other capabilities in the environment.

4.1.2 Provide Oracle expertise in supporting the configuration and operations of the environment per the standard OEM SLA identified at https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html#paas-iaas.

4.1.3 Provide Oracle IaaS environment for Test, Development and Production.

~~4.1.4 Provide confirmation of, and maintain DoD Cloud Computing Security Requirements Guide (SRG) Impact Level (IL4) minimum certification.~~
4.1.4 Use its best efforts to assist the OEM, as required by the OEM, in maintaining FedRAMP moderate and minimum DOD IL4 certification levels. The Contractor shall work with the OEM, as required by the OEM, to expeditiously maintain said certifications and shall update the Government on the status upon request and if the OEM certification status changes.

4.1.5 ~~DMDC retains ownership of any user created/loaded data and application(s) hosted on vendor's infrastructure, and maintains the right to request full copies of these at any time including access to and account information required to access all government data and government information.~~As noted in the NASA SEWP V Cloud Supplemental Terms and Conditions (STCs), DMDC and its licensors retain all ownership and intellectual property rights in and to DMDC's content. DMDC's content means all software, data (including Personal Data as that term is defined in the Data Processing Agreement), text, images, audio, video, photographs, non-Oracle or third party applications, and other content and material, in any format, provided by DMDC or any of DMDC's users that is stored in, or run on or through, the services. DMDC's content also includes any third party content that is brought by DMDC into the services, by DMDC's use of the services, or any Oracle provided tools.

DMDC is the controller of its data; as such, DMDC shall have access to its own data. At the end of the Services Period, Oracle will make DMDC's content (as it existed at the end of the Services Period) available for retrieval by DMDC during a retrieval period set out in the Service Specifications. Oracle services under this order, Oracle software, other Oracle products and services, and Oracle intellectual property, and all derivative works thereof, do not fall within the meaning of the DMDC's content. Oracle or its licensors retain all ownership and intellectual property rights to the services, derivative works thereof, and to anything developed or delivered by or on behalf of Oracle under the contract.

4.2 Software as a Service (SaaS): Provide DMDC SaaS software licenses for Oracle Fusion to meet the needs of the DCHRMS program, in accordance with the Bill of Materials

4.2.1 Renew non-production HCM Fusion environment for up to 5,000 users.

4.2.2 Within the existing Period of Performance, provide the option to continue using Shelved On Premise Licenses and receiving the Limited On Premise Support for up to an additional six (6) consecutive month period by (1) sending written notice of such election at least thirty (30) days before the end of the Initial Transition Period, and (2) providing Limited On Premise Support for such period in three-month increments (each such three-month increment is called an "Extended Transition Period" and collectively, the "Extended Transition Periods"). For each Extended Transition Period, billing will be quarterly in arrears a net fee equal to eight percent (8%) of the annual support fee for the Shelved On Premise Licenses in the most recent annual support renewal order.

4.2.3 Provide phased ability to load 900,000 total hosted employee records (but no more licenses than the government has purchased) for test purposes of the migration process prior to production implementation. Testing shall be in accordance with either (a) the already-granted Interim Authority to Test (IATT) if the cloud services being tested lack DOD SRG IL-4 or higher authorizations or (b) the relevant cloud services' DOD SRG IL-4 or higher authorizations."

4.3 Provide Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions

5.0 DELIVERABLES

Deliverable	PWS Ref.	Delivery Date
Oracle IaaS environment access for Test, Development and Production environments	4.1	Expedited, but no later than 15 days of Award
Fusion Human Capital Management Base Cloud Service (License numbers)	4.2	Expedited, but no later than 15 days of Award
All other IaaS, SaaS, as outlined in Appendices and optional CLINs	4.2	As indicated in in the Bill of Materials
Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions	4.3	Scheduling and coordination of requirements listed in the Bill of Materials to begin no later than 15 days of Award

6.0 CONTRACT ADMINISTRATION

6.1 Government Points of Contact

The identified individuals are responsible to oversee contract performance and the Contractor is responsible to coordinate with the identified individuals.

GSA Contracting Officer
Ms. Melissa DiTomaso
100 S. Independence Mall West
Philadelphia, PA 19106
Melissa.DiTomaso@gsa.gov
(215) 446-4892

GSA Contract Specialist
Mr. Katie Hughes
100 S. Independence Mall West
Philadelphia, PA 19106
katie.hughes@gsa.gov
(215)-446-4735

GSA Contracting Officer's Representative
Mr. Ruslan Gorbonos
100 S. Independence Mall West
Philadelphia, PA 19106
Ruslan.Gorbonos@gsa.gov
(215)-446-5820

DMDC COR: Will be notified Post Award

6.2 Post Award Conference

The Contractor shall participate in a Government-scheduled post-award orientation Task Order award or in accordance with Federal Acquisition Regulation Subpart 42.5. Within 7 work days of award the Contractor shall conduct an orientation briefing for the Government. The intent of the briefing is to initiate the communication process between the Government and Contractor by introducing key task participants and explaining their roles, reviewing communication ground rules, and assuring a common understanding of subtask requirements and objectives. The

Orientation Briefing's place, date and time shall be mutually agreed upon by both parties within a week from the date of award. The completion of this briefing will result in the introduction of both Contractor and Government personnel performing work under this contract. The Contractor will demonstrate confirmation of their understanding of the work to be accomplished under this SOW.

6.3 Contract Type
This is a firm fixed price task order.

6.4 Period of Performance
The period of performance is one (1) 10-month base period plus two (2) 12-month option periods.

Option periods will be exercised at the Government's unilateral right in accordance with FAR 52.217-9 - Option to Extend the Term of the Contract (Mar 2000). The government may extend the term of this contract by written notice to the contractor within thirty (30) calendar days before the contract expires; provided that the government gives the contractor a preliminary written notice of its intent to extend at least sixty (60) calendar days before the contract expires. The preliminary notice does not commit the government to an extension. If the government exercises an option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, shall not exceed thirty-four (34) months.

7.0 OTHER ADMINISTRATIVE REQUIREMENTS

7.1 ~~Records and Data~~Reserved
~~The Government will be sole owner of all technical data, any user created/loaded data and application(s) hosted on vendor's infrastructure, and maintains the right to request full copies of these at any time including access to and account information required to access all government data and government information. The Contractor shall deliver to DMDC all software, software licenses, data, form, fit and data first produced (including source code), written documents and reports to include, at a minimum, system change plans, various operations procedures and planning documents, meeting minutes, reports, manuals, training text, program management reviews, financial status reports, and any other documents created in support of this agreement or task orders. All system documentation shall be updated to remain current with each software development activity/phase. Unless otherwise stated in the orders, the Contractor shall submit deliverables to the COR or his or her designee. The Government will include review times and response to review comments in the orders. The COR will serve as DMDC's focal point for accepting the deliverables unless an order provides for other procedures.~~

7.2 Limited Use of Data
Performance of this effort may require the Contractor to access and use data and information proprietary to a Government agency or Government Contractor which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others. Consistent with the "nondisclosure" section of the NASA SEWP V Cloud Supplemental Terms and Conditions (STCs), Contractor and/or Contractor personnel shall not divulge or release data or information developed or obtained in performance of this effort, until made public by the Government, except to authorize Government personnel or upon written approval of the Contracting Officer (CO) or if required by law. The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort or as indicated in the "nondisclosure" section of the NASA SEWP V Cloud STCs. Nothing herein shall preclude the use of any data independently acquired by the Contractor without such limitations or prohibit an agreement at no cost to the Government between the Contractor and the data owner which provides for greater rights to the Contractor.

7.3 Disclosure of Information
Consistent with the "nondisclosure" section of the NASA SEWP V Cloud Supplemental Terms and Conditions (STCs), i~~I~~nformation made available to the Contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way except upon written approval of the Contracting Officer (CO) or if required by law ~~without the written agreement of the Contracting Officer~~. The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information, in accordance with the "nondisclosure" section of the NASA SEWP V Cloud STCs. Each Contractor or employee of the Contractor to whom information may be made available or disclosed shall be notified

in writing by the Contractor that such information may be disclosed only for a purpose and to the extent authorized herein.

7.4 ~~Breach Response~~Reserved

~~DoD 5400.11-R, "DoD Privacy Program," May 14, 2007, defines a breach as the "actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected." The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The Contractor shall also comply with federal laws relating to freedom of information and records management. Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access, the contractor/subcontractor shall immediately and simultaneously notify the COR, the designated Cyber Security Officer, and Privacy Officer for the contract within one (1) hour. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to DMDC assets, or sensitive information, or an action that breaches DMDC security procedures.~~

~~The Contractor shall adhere to the reporting and response requirements set forth in the Office of the Secretary of Defense (OSD) Memorandum 1504-07, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," June 5, 2009; DoD 5400.11-R, and applicable DMDC Privacy Office guidance. The Contractor shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of Protected Information by the Contractor in violation of the requirements of this Clause.~~

~~In the event of a data breach or privacy incident involving contractor processes under this contract, the Contractor shall be liable to DMDC for liquidated damages for a specified amount per affected individual to cover the cost of providing credit protection services to those individuals.~~

7.5 Invoicing

The following clauses are incorporated into the task or contract. A monthly status report shall accompany each invoice submitted in ITSS.

Clause #1 – Invoices

The Period of Performance (POP) for each invoice shall be for each quarter to align with Oracle's invoicing practices. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

1. The end of the invoiced month (for services) or
2. The end of the month in which the products (commodities) or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Cost Type, Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It shall also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, as well as the grand total of all costs incurred and invoiced.

For Cost Type, Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" for hours and dollars. Total average monthly "burn rate" may be provided in

the Monthly Status Report that accompanies the invoice. The invoice shall also include running totals for both hours and dollars.

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Note: For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items:

Charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.
- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number, task item, and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration
P.O. Box 6200-29
Portland, OR 97228-6200

Posting Acceptance Documents: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS, to allow the client and GSA COTR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following option in accepting and certifying services:

a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Task Order Number

2. Task Order ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)
10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

Final Invoice: Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COTR before payment is processed, *if necessary.*

The Government reserves the right to modify invoicing requirements at its discretion. The Contractor shall comply with any revised invoicing requirements at no additional cost to the Government

Close-out Procedures

General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

7.6 Organizational Conflict of Interest

Contractor and subcontractor personnel performing work under this contract may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

7.7 Non-Disclosure Requirements

All contractor personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the contract issued which requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit a Contractor Non-Disclosure Agreement" Form. This is required prior to the commencement of any work on such task order and whenever replacement personnel are proposed under an ongoing task order. Any information obtained or provided in the performance of this contract is only to be used in the performance of the task order. The Contractor shall take the necessary steps in accordance with Government regulations to prevent disclosure of such information to any party outside the Government and to indoctrinate its personnel who have access to sensitive information and the relationship under which the Contractor has possession of or access to the information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information will be used for the profit of any party other than those furnishing the information. The Nondisclosure Agreement for Contractor Employees shall be signed by all indoctrinated personnel and forwarded to the Contracting Officer Representative (COR) for retention, prior to work commencing. The Contractor shall restrict access to sensitive/

proprietary information to the minimum number of employees necessary for contract/Task order performance.

7.8 Security Requirements: The Contractor shall:
The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. This must include compliance with Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG), March 6, 2017 and NIST 800- 53v4.

For non-production environments, the parties agree that the Oracle Cloud Service NASA SEWP V Supplemental Terms and Conditions v033018 rev1 (STC), incorporated and attached hereto, including Oracle's Data Processing Agreement (DPA), and other service specifications (which define the administrative, physical, technical and other safeguards applied to the government's content residing in the services environment) satisfy the requirements of this section, excepting that to the extent that the STCs or DPA are precluded by Federal law (e.g., the Freedom of Information Act, the Federal Acquisition Regulation, Anti-deficiency Act, Contract Disputes Act), including and in addition to, among other things, where those documents apply foreign law (e.g., the European Union General Data Protection Regulation); permit data storage or processing outside of the United States; limit the Government's termination or dispute rights; require the Government to indemnify the Contractor or OEM; or permit the disclosure of the Government's Confidential Information; those provisions shall not apply.

Following notification by Oracle, the Contractor shall immediately communicate in writing (electronic correspondence acceptable) to the Government, any change to Oracle's FedRAMP moderate, DOD IL-4 certifications. This includes the addition or deletion of any service offerings or capabilities or changes to pricing structures.

The Contractor shall allow access only to those employees who need to perform work under this contract. The Contractor shall ensure that its employees will not discuss, divulge or disclose any information about government services to any person or entity except those persons within the Contractor's organization directly concerned with the performance of the contract.

The Contractor is responsible for ensuring employees performing work under this contract have appropriate background checks and/or vetting completed and are trustworthy to perform services under this contract.

The contractor shall report Cybersecurity incidents pertaining to government services to the government. Reporting will be done within 24 hours for root level intrusion and data compromise."~~The contractor shall report Cybersecurity incidents pertaining to government services to the government Reporting will be done within 24 hours for root level intrusion and data compromise with subsequent reporting every 24 hours until the incident is closed. The Contractor shall also notify the COR and KO at the time the incident is reported.~~

The Contractor shall not use, distribute, disclose or modify government data.

8.0 CLAUSES

- GSA Invoicing Clause
- 52.203-13 Contractor Code of Business Ethics and Conduct (OCT 2015)
- 52.204-18 Commercial and Government Entity Code Maintenance (JUL 2016)
- 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)
- 52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Dec 2019)
- 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)
- 52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015)
- 52.212-4 Contract Terms and Conditions-Commercial Items (OCT 2018)

- 52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders-Commercial Items (MAR 2020)
- 52.217-7 Option for Increased Quantity-Separately Priced Line Item (Mar 1989)
- 52.217-8 Option to Extend Services (Nov 1999)
- 52.219-6 Notice Of Total Small Business Set-Aside (MAR 2020)
- 52.219-8 Utilization of Small Business Concerns (Oct 2018)
- 52.219-13 Notice of Set-Aside of Orders (Mar 2020)
- 52.219-14 Limitations on Subcontracting (Mar 2020)
- 52.219-28 Post-Award Small Business Program Rerepresentation (Mar 2020)
- 52.224-1 Privacy Act Notification (Apr 1984)
- 52.224-2 Privacy Act (Apr 1984)
- 52.227-01 Authorization and Consent (Dec 2007)
- 52.227-19 Commercial Computer Software License (Dec 2007)
- 52.232-39 Unenforceability of Unauthorized Obligations (Jun 2013)
- 52.232-40 Providing Accelerated Payments to Small Business Subcontractors (Dec 2013)
- 52.239-1 Privacy or Security Safeguards (Aug 1996)
- 252.201-7000 CONTRACTING OFFICER'S REPRESENTATIVE (DEC 1991)
- 252.203-7002 REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (SEP 2013)
- 252.203-7003 AGENCY OFFICE OF THE INSPECTOR GENERAL (AUG 2019)
- 252.203-7005 REPRESENTATION RELATING TO COMPENSATION OF FORMER DOD OFFICIALS (NOV 2011)
- 252.204-7000 DISCLOSURE OF INFORMATION (OCT 2016)
- 252.204-7003 CONTROL OF GOVERNMENT PERSONNEL WORK PRODUCT (APR 1992)
- 252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (OCT 2016)
- 252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)
- 252.204-7016 COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES—REPRESENTATION (DEC 2019)
- 252.204-7017 PROHIBITION ON THE ACQUISITON OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES—REPRESENTATION (DEC 2019)
- 252.204-7018 PROHIBITION ON THE ACQUISITION OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES (DEC 2019)
- 252.205-7000 PROVISION OF INFORMATION TO COOPERATIVE AGREEMENT HOLDERS (DEC 1991)
- 252.215-7008 ONLY ONE OFFER (JUL 2019)
- 252.215-7013 SUPPLES AND SERVICES PROVIDED BY NONTRADITIONAL DEFENSE CONTRACTORS (JAN 2018)
- 252.227-7000 NON-ESTOPPEL (OCT 1966)
- 252.232-7007 LIMITATION OF GOVERNMENT S OBLIGATION (APR 2014)
- 252.232-7010 LEVIES ON CONTRACT PAYMENTS (DEC 2006)
- 252.239-7009 REPRESENTATION OF USE OF CLOUD COMPUTING (SEP 2015)
- 252.239-7010 CLOUD COMPUTING SERVICES (OCT 2016)
- 252.243-7001 PRICING OF CONTRACT MODIFICATIONS (DEC 1991)
- 252.243-7002 REQUESTS FOR EQUITABLE ADJUSTMENT (DEC 2012)
- 252.244-7000 SUBCONTRACTS FOR COMMERCIAL ITEMS AND COMMERCIAL COMPONENTS (DOD CONTRACTS) (JUN 2013)
- 552.216-74 Task-Order and Delivery-Order Ombudsman (Jan2017)

Statement of Work (SOW)
Defense Manpower Data Center
ORACLE Cloud Computing Services

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) located in Seaside, California has evolved into a world leader in Department of Defense (DoD) identity management, serving uniformed service members and their families across the globe. DMDC is the leader in joint information sharing and support on DoD human resource issues; the central source for identifying, authenticating, authorizing, and providing information on personnel during and after their affiliation with DoD; and the one, central access point for information and assistance on DoD entitlements, benefits, and medical readiness for uniformed service members, veterans, and their families.

2.0 BACKGROUND

DMDC is the DoD enterprise-wide provider of Humans Resource IT services and products leveraging extensive human resource focused data assets. DMDC operates the Defense Civilian Personnel Data System (DCPDS), a multifunction, web-based civilian HR information management and transaction processing system that supports approximately 900,000 civilian employee records (appropriated fund, non- appropriated fund, National Guard, and local nationals). Deployment of DCPDS began in October 1999, reaching Full Operating Capability (FOC) in September 2002. DCPDS is a global system supporting users in Asia, the Pacific, Europe and North America on a 24-hour, 7-days-a- week, basis. While DCPDS used a Commercial Off-The-Shelf (COTS) product (Oracle Enterprise Business Suite (EBS)), the system was highly-customized for the Federal and Defense environments. With over 500,000 process rules and 1.75M pay and benefit algorithm combinations, DCPDS sustains a complex set of personnel data that interfaces with the DoD payroll system and maintains over 40 other interfaces to external systems and databases. This complexity and number of interfaces resulted in increased sustainment costs and drove the need for HR reforms within the DoD.

The Reform Management Group (RMG) is a Department of Defense (DoD) decision making body comprised of Senior DoD officials with the goal of improving and streamlining the Department's business processes in accordance with the priorities that Secretary Mattis delineated in the National Defense Strategy released January 19, 2018. On May 23, 2018, the RMG, led by the Deputy Secretary of Defense (DEPSECDEF), made the decision to enable the delivery of a modern capability. That decision led to the selection of an Oracle Software as a Service (SaaS) / Human Capital Management (HCM) Cloud Platform.

In order to comply with DoD Chief Information Officer (CIO) Directives, DMDC has established a Fit for Purpose Cloud and has started migration to cloud based services and requires continued use of Oracle Cloud Infrastructure (OCI) Infrastructure-as-a-Service (IaaS) in order to provide a highly-reliable, scalable and low-cost infrastructure platform in the cloud that offers DMDC users the ability to utilize, stand up and take down IT infrastructure (both programs and platforms) on demand. The on-demand nature of commercial cloud services reduces the necessity for DMDC users to expend the time and resources required to procure, sustain and maintain IT infrastructure which may only be needed for limited periods of time.

The Defense Civilian Human Resources Management System (DCHRMS) will replace the DCPDS, and move the Human Resources (HR) information system (HRIS) from six separate databases that maintain DoD employee records into one integrated enterprise database. DCHRMS is a Human Resource (HR) information system (HRIS) that will support civilian HR management, establish a single employee record, and create standardized personnel data across the enterprise. It is a cloud-based system that built on Oracle's Fusion HCM Base Cloud Software as a Service to provide a single civilian personnel service capability for the DoD.

DMDC has utilized OCI services for over a year. In that time, DMDC has migrated its Civilian Personnel IT Portfolio into OCI and is ready to expand the DMDC Fit for Purpose Cloud for additional DMDC portfolios by utilizing OCI services such as: compute, storage, databases, logging and monitoring, capacity management and provisioning, high-speed computing/analytics, virtual private cloud and web hosting to complete the transition out of the On-Premise data

centers into a Cloud environment per DoD guidance.

This requirement is a continuing effort to migrate DMDC applications from the data centers located in Seaside, CA and Columbus, OH to OCI in accordance with DoD CIO mandated Data Center Closure Guidance and includes cloud-based services to continue hosting the Department of Defense's (DoD) Civilian HR Information Technology (IT) portfolio, aligning with Federal and DoD initiatives, specifically the DoD CIO approved Business Case Analysis (BCA). Additionally, in order to prepare for the operational version of the DCHRMS program, the government must continue the subscription to Oracle Fusion of one license per user, a total of 900,000 Oracle Fusion licenses prior to full deployment.

The Oracle Cloud Service Offering will provide the next generation transactional Civilian HR system, DCHRMS, in a commercial-based HCM Solution along with the infrastructure for additional capabilities required to meet the DMDC mission. The Oracle HCM/Fusion Software licenses and technical support will replace the current Defense Civilian Personnel Data System (DCPDS) while the Oracle Cloud Infrastructure (OCI) will host the other existing applications.

3.0 SCOPE

This requirement focuses on the hosting of persistent Non-classified Internet Protocol (IP) Router Network (NIPRNet) systems currently hosted at the DMDC enclave at the Columbus, OH Defense Enterprise Computing Center (DECC) and the Seaside, CA Defense Manpower Data Center; continued hosting of the DoD Civilian HR IT portfolio; Oracle HCM SaaS; software licenses; technical support and Oracle University instructor led training for use of the HCM Cloud as well as Reporting Analytics. The Contractor shall provide the materials and space necessary to accomplish Oracle Cloud Infrastructure-as-a-Service (IaaS) environment and support necessary for cloud services: compute, storage, databases, logging and monitoring, capacity management and provisioning, high-speed computing/analytics, virtual private cloud and web hosting per the standard Service Level Agreements (SLA). The Contractor must be an authorized brand reseller of Oracle at the Gold or Platinum Partner level and the Cloud Service Offering (CSO) must be certified at the DoD Cloud Computing Security Requirements Guide (SRG) Impact Level 4 (IL4) or above.

In addition to OCI IaaS for the Fit for Purpose Cloud, DMDC requires Oracle SaaS environment space; user licenses infrastructure, and technical support to continue to operate its Civilian Personnel IT Portfolio and its next generation transactional Human Resources (HR) System, the Defense Civilian Human Resources Management System (DCHRMS), in a commercial-based Human Capital Management (HCM) Solution. The DCHRMS system is required to be operational within the Oracle Fusion SaaS environment.

DMDC also requires Oracle Fusion Software and licenses including DCHRMS Performance and Goal Management licenses; and DCPDS EBS maintenance to continue the operation of the DCHRMS Human Capital Management (HCM) environment as well as space in the OCI Oracle IaaS environment with the technical services to assist DMDC to accomplish the migration of all remaining applications from the Seaside and Columbus Data Centers.

Lastly, DMDC requires Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions.

4.0 REQUIREMENTS *The Contractor shall*:

4.1 Infrastructure as a Service (IaaS): Provide IaaS within the Oracle Cloud Infrastructure (OCI) environment in accordance with the Bill of Materials. Performance includes at a minimum:

4.1.1 Provide Compute, Storage, Network, Database Backup, Disaster Recovery, and other capabilities in the environment.

4.1.2 Provide Oracle expertise in supporting the configuration and operations of the environment per the standard OEM SLA identified at https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html#paas-iaas.

4.1.3 Provide Oracle IaaS environment for Test, Development and Production.

4.1.4 Use its best efforts to assist the OEM, as required by the OEM, in maintaining FedRAMP moderate and minimum DOD IL4 certification levels. The Contractor shall work with the OEM, as required by the OEM, to expeditiously maintain said certifications and shall update the Government on the status upon request and if the OEM certification status changes.

4.1.5 As noted in the NASA SEWP V Cloud Supplemental Terms and Conditions (STCs), DMDC and its licensors retain all ownership and intellectual property rights in and to DMDC's content. DMDC's content means all software, data (including Personal Data as that term is defined in the Data Processing Agreement), text, images, audio, video, photographs, non-Oracle or third party applications, and other content and material, in any format, provided by DMDC or any of DMDC's users that is stored in, or run on or through, the services. DMDC's content also includes any third party content that is brought by DMDC into the services, by DMDC's use of the services, or any Oracle provided tools.

DMDC is the controller of its data; as such, DMDC shall have access to its own data. At the end of the Services Period, Oracle will make DMDC's content (as it existed at the end of the Services Period) available for retrieval by DMDC during a retrieval period set out in the Service Specifications. Oracle services under this order, Oracle software, other Oracle products and services, and Oracle intellectual property, and all derivative works thereof, do not fall within the meaning of the DMDC's content. Oracle or its licensors retain all ownership and intellectual property rights to the services, derivative works thereof, and to anything developed or delivered by or on behalf of Oracle under the contract.

4.2 Software as a Service (SaaS): Provide DMDC SaaS software licenses for Oracle Fusion to meet the needs of the DCHRMS program, in accordance with the Bill of Materials

4.2.1 Renew non-production HCM Fusion environment for up to 5,000 users.

4.2.2 Within the existing Period of Performance, provide the option to continue using Shelved On Premise Licenses and receiving the Limited On Premise Support for up to an additional six (6) consecutive month period by (1) sending written notice of such election at least thirty (30) days before the end of the Initial Transition Period, and (2) providing Limited On Premise Support for such period in three-month increments (each such three-month increment is called an "Extended Transition Period" and collectively, the "Extended Transition Periods"). For each Extended Transition Period, billing will be quarterly in arrears a net fee equal to eight percent (8%) of the annual support fee for the Shelved On Premise Licenses in the most recent annual support renewal order.

4.2.3 Provide phased ability to load 900,000 total hosted employee records (but no more licenses than the government has purchased) for test purposes of the migration process prior to production implementation. Testing shall be in accordance with either (a) the already-granted Interim Authority to Test (IATT) if the cloud services being tested lack DOD SRG IL-4 or higher authorizations or (b) the relevant cloud services' DOD SRG IL-4 or higher authorizations."

4.3 Provide Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions

5.0 DELIVERABLES

Deliverable	PWS Ref.	Delivery Date

Oracle IaaS environment access for Test, Development and Production environments	4.1	Expedited, but no later than 15 days of Award
Fusion Human Capital Management Base Cloud Service (License numbers)	4.2	Expedited, but no later than 15 days of Award
All other IaaS, SaaS, as outlined in Appendices and optional CLINs	4.2	As indicated in in the Bill of Materials
Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions	4.3	Scheduling and coordination of requirements listed in the Bill of Materials to begin no later than 15 days of Award

6.0 CONTRACT ADMINISTRATION

6.1 Government Points of Contact

The identified individuals are responsible to oversee contract performance and the Contractor is responsible to coordinate with the identified individuals.

GSA Contracting Officer
Ms. Melissa DiTomaso
100 S. Independence Mall West
Philadelphia, PA 19106
Melissa.DiTomaso@gsa.gov
(215) 446-4892

GSA Contract Specialist
Mr. Katie Hughes
100 S. Independence Mall West
Philadelphia, PA 19106
katie.hughes@gsa.gov
(215)-446-4735

GSA Contracting Officer's Representative
Mr. Ruslan Gorbonos
100 S. Independence Mall West
Philadelphia, PA 19106
Ruslan.Gorbonos@gsa.gov
(215)-446-5820

DMDC COR: Will be notified Post Award

6.2 Post Award Conference

The Contractor shall participate in a Government-scheduled post-award orientation Task Order award or in accordance with Federal Acquisition Regulation Subpart 42.5. Within 7 work days of award the Contractor shall conduct an orientation briefing for the Government. The intent of the briefing is to initiate the communication process between the Government and Contractor by introducing key task participants and explaining their roles, reviewing communication ground rules, and assuring a common understanding of subtask requirements and objectives. The Orientation Briefing's place, date and time shall be mutually agreed upon by both parties within a week from the date of award. The completion of this briefing will result in the introduction of both Contractor and Government personnel performing work under this contract. The Contractor will demonstrate confirmation of their understanding of the work to be accomplished under this SOW.

6.3 Contract Type
This is a firm fixed price task order.

6.4 Period of Performance
The period of performance is one (1) 10-month base period plus two (2) 12-month option periods.

Option periods will be exercised at the Government's unilateral right in accordance with FAR 52.217-9 - Option to Extend the Term of the Contract (Mar 2000). The government may extend the term of this contract by written notice to the contractor within thirty (30) calendar days before the contract expires; provided that the government gives the contractor a preliminary written notice of its intent to extend at least sixty (60) calendar days before the contract expires. The preliminary notice does not commit the government to an extension. If the government exercises an option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, shall not exceed thirty-four (34) months.

7.0 OTHER ADMINISTRATIVE REQUIREMENTS
7.1 Reserved

7.2 Limited Use of Data
Performance of this effort may require the Contractor to access and use data and information proprietary to a Government agency or Government Contractor which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others. Consistent with the "nondisclosure" section of the NASA SEWP V Cloud Supplemental Terms and Conditions (STCs), Contractor and/or Contractor personnel shall not divulge or release data or information developed or obtained in performance of this effort, until made public by the Government, except to authorize Government personnel or upon written approval of the Contracting Officer (CO) or if required by law. The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort or as indicated in the "nondisclosure" section of the NASA SEWP V Cloud STCs. Nothing herein shall preclude the use of any data independently acquired by the Contractor without such limitations or prohibit an agreement at no cost to the Government between the Contractor and the data owner which provides for greater rights to the Contractor.

7.3 Disclosure of Information
Consistent with the "nondisclosure" section of the NASA SEWP V Cloud Supplemental Terms and Conditions (STCs), information made available to the Contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way except upon written approval of the Contracting Officer (CO) or if required by law . The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information, in accordance with the "nondisclosure" section of the NASA SEWP V Cloud STCs. Each Contractor or employee of the Contractor to whom information may be made available or disclosed shall be notified in writing by the Contractor that such information may be disclosed only for a purpose and to the extent authorized herein.

7.4 Reserved

7.5 Invoicing

The following clauses are incorporated into the task or contract. A monthly status report shall accompany each invoice submitted in ITSS.

Clause #1 – Invoices

The Period of Performance (POP) for each invoice shall be for each quarter to align with Oracle's invoicing practices. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

1. The end of the invoiced month (for services) or

2. The end of the month in which the products (commodities) or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Cost Type, Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It shall also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, as well as the grand total of all costs incurred and invoiced.

For Cost Type, Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" for hours and dollars. Total average monthly "burn rate" may be provided in the Monthly Status Report that accompanies the invoice. The invoice shall also include running totals for both hours and dollars.

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Note: For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items:

Charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.
- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number, task item, and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration
P.O. Box 6200-29
Portland, OR 97228-6200

Posting Acceptance Documents: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS, to allow the client and GSA COTR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following option in accepting and certifying services:

a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Task Order Number
2. Task Order ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)
10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

Final Invoice: Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COTR before payment is processed, *if necessary*.

The Government reserves the right to modify invoicing requirements at its discretion. The Contractor shall comply with any revised invoicing requirements at no additional cost to the Government

Close-out Procedures

General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

7.6 Organizational Conflict of Interest

Contractor and subcontractor personnel performing work under this contract may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

7.7 Non-Disclosure Requirements

All contractor personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the contract issued which requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and

submit a Contractor Non-Disclosure Agreement" Form. This is required prior to the commencement of any work on such task order and whenever replacement personnel are proposed under an ongoing task order. Any information obtained or provided in the performance of this contract is only to be used in the performance of the task order. The Contractor shall take the necessary steps in accordance with Government regulations to prevent disclosure of such information to any party outside the Government and to indoctrinate its personnel who have access to sensitive information and the relationship under which the Contractor has possession of or access to the information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information will be used for the profit of any party other than those furnishing the information. The Nondisclosure Agreement for Contractor Employees shall be signed by all indoctrinated personnel and forwarded to the Contracting Officer Representative (COR) for retention, prior to work commencing. The Contractor shall restrict access to sensitive/ proprietary information to the minimum number of employees necessary for contract/Task order performance.

7.8 Security Requirements: The Contractor shall:
The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. This must include compliance with Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG), March 6, 2017 and NIST 800- 53v4.

For non-production environments, the parties agree that the Oracle Cloud Service NASA SEWP V Supplemental Terms and Conditions v033018 rev1 (STC), incorporated and attached hereto, including Oracle's Data Processing Agreement (DPA), and other service specifications (which define the administrative, physical, technical and other safeguards applied to the government's content residing in the services environment) satisfy the requirements of this section, excepting that to the extent that the STCs or DPA are precluded by Federal law (e.g., the Freedom of Information Act, the Federal Acquisition Regulation, Anti-deficiency Act, Contract Disputes Act), including and in addition to, among other things, where those documents apply foreign law (e.g., the European Union General Data Protection Regulation); permit data storage or processing outside of the United States; limit the Government's termination or dispute rights; require the Government to indemnify the Contractor or OEM; or permit the disclosure of the Government's Confidential Information; those provisions shall not apply.

Following notification by Oracle, the Contractor shall immediately communicate in writing (electronic correspondence acceptable) to the Government, any change to Oracle's FedRAMP moderate, DOD IL-4 certifications. This includes the addition or deletion of any service offerings or capabilities or changes to pricing structures.

The Contractor shall allow access only to those employees who need to perform work under this contract. The Contractor shall ensure that its employees will not discuss, divulge or disclose any information about government services to any person or entity except those persons within the Contractor's organization directly concerned with the performance of the contract.

The Contractor is responsible for ensuring employees performing work under this contract have appropriate background checks and/or vetting completed and are trustworthy to perform services under this contract.

The contractor shall report Cybersecurity incidents pertaining to government services to the government. Reporting will be done within 24 hours for root level intrusion and data compromise."
The Contractor shall not use, distribute, disclose or modify government data.

8.0 CLAUSES

- GSA Invoicing Clause
- 52.203-13 Contractor Code of Business Ethics and Conduct (OCT 2015)
- 52.204-18 Commercial and Government Entity Code Maintenance (JUL 2016)
- 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)

- 52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Dec 2019)
- 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)
- 52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015)
- 52.212-4 Contract Terms and Conditions-Commercial Items (OCT 2018)
- 52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders-Commercial Items (MAR 2020)
- 52.217-7 Option for Increased Quantity-Separately Priced Line Item (Mar 1989)
- 52.217-8 Option to Extend Services (Nov 1999)
- 52.219-6 Notice Of Total Small Business Set-Aside (MAR 2020)
- 52.219-8 Utilization of Small Business Concerns (Oct 2018)
- 52.219-13 Notice of Set-Aside of Orders (Mar 2020)
- 52.219-14 Limitations on Subcontracting (Mar 2020)
- 52.219-28 Post-Award Small Business Program Rerepresentation (Mar 2020)
- 52.224-1 Privacy Act Notification (Apr 1984)
- 52.224-2 Privacy Act (Apr 1984)
- 52.227-01 Authorization and Consent (Dec 2007)
- 52.227-19 Commercial Computer Software License (Dec 2007)
- 52.232-39 Unenforceability of Unauthorized Obligations (Jun 2013)
- 52.232-40 Providing Accelerated Payments to Small Business Subcontractors (Dec 2013)
- 52.239-1 Privacy or Security Safeguards (Aug 1996)
- 252.201-7000 CONTRACTING OFFICER'S REPRESENTATIVE (DEC 1991)
- 252.203-7002 REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (SEP 2013)
- 252.203-7003 AGENCY OFFICE OF THE INSPECTOR GENERAL (AUG 2019)
- 252.203-7005 REPRESENTATION RELATING TO COMPENSATION OF FORMER DOD OFFICIALS (NOV 2011)
- 252.204-7000 DISCLOSURE OF INFORMATION (OCT 2016)
- 252.204-7003 CONTROL OF GOVERNMENT PERSONNEL WORK PRODUCT (APR 1992)
- 252.204-7008 COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016)
- 252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (OCT 2016)
- 252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)
- 252.204-7016 COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES—REPRESENTATION (DEC 2019)
- 252.204-7017 PROHIBITION ON THE ACQUISITON OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES—REPRESENTATION (DEC 2019)
- 252.204-7018 PROHIBITION ON THE ACQUISITION OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES (DEC 2019)
- 252.205-7000 PROVISION OF INFORMATION TO COOPERATIVE AGREEMENT HOLDERS (DEC 1991)
- 252.215-7008 ONLY ONE OFFER (JUL 2019)
- 252.215-7013 SUPPLES AND SERVICES PROVIDED BY NONTRADITIONAL DEFENSE CONTRACTORS (JAN 2018)
- 252.227-7000 NON-ESTOPPEL (OCT 1966)
- 252.232-7007 LIMITATION OF GOVERNMENT S OBLIGATION (APR 2014)
- 252.232-7010 LEVIES ON CONTRACT PAYMENTS (DEC 2006)
- 252.239-7009 REPRESENTATION OF USE OF CLOUD COMPUTING (SEP 2015)
- 252.239-7010 CLOUD COMPUTING SERVICES (OCT 2016)

- 252.243-7001 PRICING OF CONTRACT MODIFICATIONS (DEC 1991)
- 252.243-7002 REQUESTS FOR EQUITABLE ADJUSTMENT (DEC 2012)
- 252.244-7000 SUBCONTRACTS FOR COMMERCIAL ITEMS AND COMMERCIAL COMPONENTS (DOD CONTRACTS) (JUN 2013)
- 552.216-74 Task-Order and Delivery-Order Ombudsman (Jan2017)

Statement of Work (SOW)
Defense Manpower Data Center
ORACLE Cloud Computing Services

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) located in Seaside, California has evolved into a world leader in Department of Defense (DoD) identity management, serving uniformed service members and their families across the globe. DMDC is the leader in joint information sharing and support on DoD human resource issues; the central source for identifying, authenticating, authorizing, and providing information on personnel during and after their affiliation with DoD; and the one, central access point for information and assistance on DoD entitlements, benefits, and medical readiness for uniformed service members, veterans, and their families.

2.0 BACKGROUND

DMDC is the DoD enterprise-wide provider of Humans Resource IT services and products leveraging extensive human resource focused data assets. DMDC operates the Defense Civilian Personnel Data System (DCPDS), a multifunction, web-based civilian HR information management and transaction processing system that supports approximately 900,000 civilian employee records (appropriated fund, non- appropriated fund, National Guard, and local nationals). Deployment of DCPDS began in October 1999, reaching Full Operating Capability (FOC) in September 2002. DCPDS is a global system supporting users in Asia, the Pacific, Europe and North America on a 24-hour, 7-days-a- week, basis. While DCPDS used a Commercial Off-The-Shelf (COTS) product (Oracle Enterprise Business Suite (EBS)), the system was highly-customized for the Federal and Defense environments. With over 500,000 process rules and 1.75M pay and benefit algorithm combinations, DCPDS sustains a complex set of personnel data that interfaces with the DoD payroll system and maintains over 40 other interfaces to external systems and databases. This complexity and number of interfaces resulted in increased sustainment costs and drove the need for HR reforms within the DoD.

The Reform Management Group (RMG) is a Department of Defense (DoD) decision making body comprised of Senior DoD officials with the goal of improving and streamlining the Department's business processes in accordance with the priorities that Secretary Mattis delineated in the National Defense Strategy released January 19, 2018. On May 23, 2018, the RMG, led by the Deputy Secretary of Defense (DEPSECDEF), made the decision to enable the delivery of a modern capability. That decision led to the selection of an Oracle Software as a Service (SaaS) / Human Capital Management (HCM) Cloud Platform.

In order to comply with DoD Chief Information Officer (CIO) Directives, DMDC has established a Fit for Purpose Cloud and has started migration to cloud based services and requires continued use of Oracle Cloud Infrastructure (OCI) Infrastructure-as-a-Service (IaaS) in order to provide a highly-reliable, scalable and low-cost infrastructure platform in the cloud that offers DMDC users the ability to utilize, stand up and take down IT infrastructure (both programs and platforms) on demand. The on-demand nature of commercial cloud services reduces the necessity for DMDC users to expend the time and resources required to procure, sustain and maintain IT infrastructure which may only be needed for limited periods of time.

The Defense Civilian Human Resources Management System (DCHRMS) will replace the DCPDS, and move the Human Resources (HR) information system (HRIS) from six separate databases that maintain DoD employee records into one integrated enterprise database. DCHRMS is a Human Resource (HR) information system (HRIS) that will support civilian HR management, establish a single employee record, and create standardized personnel data across the enterprise. It is a cloud-based system that built on Oracle's Fusion HCM Base Cloud Software as a Service to provide a single civilian personnel service capability for the DoD.

DMDC has utilized OCI services for over a year. In that time, DMDC has migrated its Civilian Personnel IT Portfolio into OCI and is ready to expand the DMDC Fit for Purpose Cloud for additional DMDC portfolios by utilizing OCI services such as: compute, storage, databases, logging and monitoring, capacity management and provisioning, high-speed computing/analytics, virtual private cloud and web hosting to complete the transition out of the On-Premise data

centers into a Cloud environment per DoD guidance.

This requirement is a continuing effort to migrate DMDC applications from the data centers located in Seaside, CA and Columbus, OH to OCI in accordance with DoD CIO mandated Data Center Closure Guidance and includes cloud-based services to continue hosting the Department of Defense's (DoD) Civilian HR Information Technology (IT) portfolio, aligning with Federal and DoD initiatives, specifically the DoD CIO approved Business Case Analysis (BCA). Additionally, in order to prepare for the operational version of the DCHRMS program, the government must continue the subscription to Oracle Fusion of one license per user, a total of 900,000 Oracle Fusion licenses prior to full deployment.

The Oracle Cloud Service Offering will provide the next generation transactional Civilian HR system, DCHRMS, in a commercial-based HCM Solution along with the infrastructure for additional capabilities required to meet the DMDC mission. The Oracle HCM/Fusion Software licenses and technical support will replace the current Defense Civilian Personnel Data System (DCPDS) while the Oracle Cloud Infrastructure (OCI) will host the other existing applications.

3.0 SCOPE

This requirement focuses on the hosting of persistent Non-classified Internet Protocol (IP) Router Network (NIPRNet) systems currently hosted at the DMDC enclave at the Columbus, OH Defense Enterprise Computing Center (DECC) and the Seaside, CA Defense Manpower Data Center; continued hosting of the DoD Civilian HR IT portfolio; Oracle HCM SaaS; software licenses; technical support and Oracle University instructor led training for use of the HCM Cloud as well as Reporting Analytics. The Contractor shall provide the materials and space necessary to accomplish Oracle Cloud Infrastructure-as-a-Service (IaaS) environment and support necessary for cloud services: compute, storage, databases, logging and monitoring, capacity management and provisioning, high-speed computing/analytics, virtual private cloud and web hosting per the standard Service Level Agreements (SLA). The Contractor must be an authorized brand reseller of Oracle at the Gold or Platinum Partner level and the Cloud Service Offering (CSO) must be certified at the DoD Cloud Computing Security Requirements Guide (SRG) Impact Level 4 (IL4) or above.

In addition to OCI IaaS for the Fit for Purpose Cloud, DMDC requires Oracle SaaS environment space; user licenses infrastructure, and technical support to continue to operate its Civilian Personnel IT Portfolio and its next generation transactional Human Resources (HR) System, the Defense Civilian Human Resources Management System (DCHRMS), in a commercial-based Human Capital Management (HCM) Solution. The DCHRMS system is required to be operational within the Oracle Fusion SaaS environment.

DMDC also requires Oracle Fusion Software and licenses including DCHRMS Performance and Goal Management licenses; and DCPDS EBS maintenance to continue the operation of the DCHRMS Human Capital Management (HCM) environment as well as space in the OCI Oracle IaaS environment with the technical services to assist DMDC to accomplish the migration of all remaining applications from the Seaside and Columbus Data Centers.

Lastly, DMDC requires Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions.

4.0 REQUIREMENTS *The Contractor shall*:

4.1 Infrastructure as a Service (IaaS): Provide IaaS within the Oracle Cloud Infrastructure (OCI) environment. Performance includes at a minimum:

4.1.1 Provide Compute, Storage, Network, Database Backup, Disaster Recovery, and other capabilities in the environment.

4.1.2 Provide Oracle expertise in supporting the configuration and operations of the environment per the standard OEM SLA identified at https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html#paas-iaas. If Oracle enhances the SLAs post award, such SLA shall apply to this order without additional cost to the Government.

4.1.3 Provide Oracle IaaS environment for Test, Development and Production.

4.1.4 Provide confirmation of, and maintain DoD Cloud Computing Security Requirements Guide (SRG) Impact Level (IL4) certification.

4.1.5 DMDC retains ownership of any user created/loaded data and application(s) hosted on vendor's infrastructure, and maintains the right to request full copies of these at any time including access to and account information required to access all government data and government information.

4.2 Software as a Service (SaaS): Provide DMDC SaaS software licenses for Oracle Fusion to meet the needs of the DCHRMS program.

4.2.1 Renew non-production HCM Fusion environment for up to 5,000 users.

4.2.2 Provide the option to continue using Shelved On Premise Licenses and receiving the Limited On Premise Support for up to an additional six (6) consecutive month period by (1) sending written notice of such election at least thirty (30) days before the end of the Initial Transition Period, and (2) providing Limited On Premise Support for such period in three-month increments (each such three-month increment is called an "Extended Transition Period" and collectively, the "Extended Transition Periods"). For each Extended Transition Period, billing will be quarterly in arrears a net fee equal to eight percent (8%) of the annual support fee for the Shelved On Premise Licenses in the most recent annual support renewal order.

4.2.3 Provide phased ability to load 900,000 total hosted employee records (but no more licenses than the government has purchased) for test purposes of the migration process prior to production implementation. Testing shall be in accordance with granted Interim Authority to Test (IATT).

4.3 Provide Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions

5.0 DELIVERABLES

Deliverable	PWS Ref.	Delivery Date
Oracle IaaS environment access for Test, Development and Production environments	4.1	Expedited, but no later than 15 days of Award
Fusion Human Capital Management Base Cloud Service (License numbers)	4.2	Expedited, but no later than 15 days of Award
All other IaaS, SaaS, as outlined in Appendices and optional CLINs	4.2	As indicated in in the Bill of Materials
Oracle University Instructor-led training for the use of the HCM Cloud and Reporting Analytics functions	4.3	Scheduling and coordination of requirements listed in the Bill of Materials to begin no later than 15 days of Award

6.0 CONTRACT ADMINISTRATION

6.1 Government Points of Contact

The identified individuals are responsible to oversee contract performance and the Contractor is responsible to coordinate with the identified individuals.

GSA Contracting Officer
Ms. Melissa DiTomaso
100 S. Independence Mall West
Philadelphia, PA 19106
Melissa.DiTomaso@gsa.gov
(215) 446-4892

GSA Contract Specialist
Mr. Katie Hughes
100 S. Independence Mall West
Philadelphia, PA 19106
katie.hughes@gsa.gov
(215)-446-4735

GSA Contracting Officer's Representative
Mr. Ruslan Gorbonos
100 S. Independence Mall West
Philadelphia, PA 19106
Ruslan.Gorbonos@gsa.gov
(215)-446-5820

DMDC COR: Will be notified Post Award

6.2 Post Award Conference
The Contractor shall participate in a Government-scheduled post-award orientation Task Order award or in accordance with Federal Acquisition Regulation Subpart 42.5. Within 7 work days of award the Contractor shall conduct an orientation briefing for the Government. The intent of the briefing is to initiate the communication process between the Government and Contractor by introducing key task participants and explaining their roles, reviewing communication ground rules, and assuring a common understanding of subtask requirements and objectives. The Orientation Briefing's place, date and time shall be mutually agreed upon by both parties within a week from the date of award. The completion of this briefing will result in the introduction of both Contractor and Government personnel performing work under this contract. The Contractor will demonstrate confirmation of their understanding of the work to be accomplished under this SOW.

6.3 Contract Type
This is a firm fixed price task order.

6.4 Period of Performance
The period of performance is one (1) 11-month base period plus two (2) 12-month option periods.

Option periods will be exercised at the Government's unilateral right in accordance with FAR 52.217-9 - Option to Extend the Term of the Contract (Mar 2000). The government may extend the term of this contract by written notice to the contractor within thirty (30) calendar days before the contract expires; provided that the government gives the contractor a preliminary written notice of its intent to extend at least sixty (60) calendar days before the contract expires. The preliminary notice does not commit the government to an extension. If the government exercises an option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, shall not exceed sixty (60) months.

7.0 OTHER ADMINISTRATIVE REQUIREMENTS

7.1 Records and Data
The Government will be sole owner of all technical data, software developed, and infrastructure designed under this project. The Contractor shall deliver to DMDC all software, software licenses, data, form, fit and data first produced (including source code), written documents and reports to include, at a minimum, system change plans, various

operations procedures and planning documents, meeting minutes, reports, manuals, training text, program management reviews, financial status reports, and any other documents created in support of this agreement or task orders. All system documentation shall be updated to remain current with each software development activity/phase. Unless otherwise stated in the orders, the Contractor shall submit deliverables to the COR or his or her designee. The Government will include review times and response to review comments in the orders. The COR will serve as DMDC's focal point for accepting the deliverables unless an order provides for other procedures.

7.2 Limited Use of Data

Performance of this effort may require the Contractor to access and use data and information proprietary to a Government agency or Government Contractor which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others. Contractor and/or Contractor personnel shall not divulge or release data or information developed or obtained in performance of this effort, until made public by the Government, except to authorize Government personnel or upon written approval of the Contracting Officer (CO). The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort. Nothing herein shall preclude the use of any data independently acquired by the Contractor without such limitations or prohibit an agreement at no cost to the Government between the Contractor and the data owner which provides for greater rights to the Contractor.

7.3 Disclosure of Information

Information made available to the Contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way without the written agreement of the Contracting Officer. The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information. Each Contractor or employee of the Contractor to whom information may be made available or disclosed shall be notified in writing by the Contractor that such information may be disclosed only for a purpose and to the extent authorized herein.

7.4 Breach Response

DoD 5400.11-R, "DoD Privacy Program," May 14, 2007, defines a breach as the "actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected." The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The Contractor shall also comply with federal laws relating to freedom of information and records management. Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access, the contractor/subcontractor shall immediately and simultaneously notify the COR, the designated Cyber Security Officer, and Privacy Officer for the contract within one (1) hour. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to DMDC assets, or sensitive information, or an action that breaches DMDC security procedures.

The Contractor shall adhere to the reporting and response requirements set forth in the Office of the Secretary of Defense (OSD) Memorandum 1504-07, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," June 5, 2009; DoD 5400.11-R, and applicable DMDC Privacy Office guidance. The Contractor shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of Protected Information by the Contractor in violation of the requirements of this Clause.
In the event of a data breach or privacy incident involving contractor processes under this contract, the Contractor shall be liable to DMDC for liquidated damages for a specified amount per affected individual to cover the cost of providing credit protection services to those individuals.

7.5 Invoicing

The following clauses are incorporated into the task or contract. A monthly status report shall accompany each invoice submitted in ITSS.

Clause #1 – Invoices

The Period of Performance (POP) for each invoice shall be for one calendar month. The contractor shall submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

1. The end of the invoiced month (for services) or
2. The end of the month in which the products (commodities) or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Cost Type, Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It shall also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, as well as the grand total of all costs incurred and invoiced.

For Cost Type, Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" for hours and dollars. Total average monthly "burn rate" may be provided in the Monthly Status Report that accompanies the invoice. The invoice shall also include running totals for both hours and dollars.

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Note: For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items:

Charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.
- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number, task item, and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration

P.O. Box 6200-29
Portland, OR 97228-6200

Posting Acceptance Documents: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS, to allow the client and GSA COTR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following option in accepting and certifying services:

a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Task Order Number
2. Task Order ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)
10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

Final Invoice: Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COTR before payment is processed, *if necessary.*

The Government reserves the right to modify invoicing requirements at its discretion. The Contractor shall comply with any revised invoicing requirements at no additional cost to the Government

Close-out Procedures
General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

7.6 Organizational Conflict of Interest

Contractor and subcontractor personnel performing work under this contract may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in

any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

7.7 Non-Disclosure Requirements

All contractor personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the contract issued which requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit a Contractor Non-Disclosure Agreement" Form. This is required prior to the commencement of any work on such task order and whenever replacement personnel are proposed under an ongoing task order. Any information obtained or provided in the performance of this contract is only to be used in the performance of the task order. The Contractor shall take the necessary steps in accordance with Government regulations to prevent disclosure of such information to any party outside the Government and to indoctrinate its personnel who have access to sensitive information and the relationship under which the Contractor has possession of or access to the information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information will be used for the profit of any party other than those furnishing the information. The Nondisclosure Agreement for Contractor Employees shall be signed by all indoctrinated personnel and forwarded to the Contracting Officer Representative (COR) for retention, prior to work commencing. The Contractor shall restrict access to sensitive/ proprietary information to the minimum number of employees necessary for contract/Task order performance.

7.8 Security Requirements: The Contractor shall:

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. This must include compliance with Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG), March 6, 2017 and NIST 800- 53v4.

For non-production environments, the parties agree that the Oracle Cloud Service NASA SEWP V Supplemental Terms and Conditions v033018 rev1 (STC), incorporated and attached hereto, including Oracle's Data Processing Agreement (DPA), and other service specifications (which define the administrative, physical, technical and other safeguards applied to the government's content residing in the services environment) satisfy the requirements of this section, excepting that to the extent that the STCs or DPA are precluded by Federal law (e.g., the Freedom of Information Act, the Federal Acquisition Regulation, Anti-deficiency Act, Contract Disputes Act), including and in addition to, among other things, where those documents apply foreign law (e.g., the European Union General Data Protection Regulation); permit data storage or processing outside of the United States; limit the Government's termination or dispute rights; require the Government to indemnify the Contractor or OEM; or permit the disclosure of the Government's Confidential Information; those provisions shall not apply.

Following notification by Oracle, the Contractor shall immediately communicate in writing (electronic correspondence acceptable) to the Government, any change to Oracle's FedRAMP moderate, DOD IL-4 certifications. This includes the addition or deletion of any service offerings or capabilities or changes to pricing structures.

The Contractor shall allow access only to those employees who need to perform work under this contract. The Contractor shall ensure that its employees will not discuss, divulge or disclose any information about government services to any person or entity except those persons within the Contractor's organization directly concerned with the performance of the contract.

The Contractor is responsible for ensuring employees performing work under this contract have appropriate background checks and/or vetting completed and are trustworthy to perform services under this contract.

The contractor shall report Cybersecurity incidents pertaining to government services to the government within one

(1) hour of discovery. Reporting will be done within 24 hours for root level intrusion and data compromise with subsequent reporting every 24 hours until the incident is closed. The Contractor shall also notify the COR and KO at the time the incident is reported.

The Contractor shall not use, distribute, disclose or modify government data.

8.0 CLAUSES

- GSA Invoicing Clause

- 52.203-13 Contractor Code of Business Ethics and Conduct (OCT 2015)
- 52.204-18 Commercial and Government Entity Code Maintenance (JUL 2016)
- 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)
- 52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Dec 2019)
- 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)
- 52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015)
- 52.212-4 Contract Terms and Conditions-Commercial Items (OCT 2018)
- 52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders-Commercial Items (MAR 2020)
- 52.217-7 Option for Increased Quantity-Separately Priced Line Item (Mar 1989)
- 52.217-8 Option to Extend Services (Nov 1999)
- 52.219-6 Notice Of Total Small Business Set-Aside (MAR 2020)
- 52.219-8 Utilization of Small Business Concerns (Oct 2018)
- 52.219-13 Notice of Set-Aside of Orders (Mar 2020)
- 52.219-14 Limitations on Subcontracting (Mar 2020)
- 52.219-28 Post-Award Small Business Program Rerepresentation (Mar 2020)
- 52.223-16 Acquisition of EPEAT®-Registered Personal Computer Products (Oct 2015)
- 52.224-1 Privacy Act Notification (Apr 1984)
- 52.224-2 Privacy Act (Apr 1984)
- 52.227-01 Authorization and Consent (Dec 2007)
- 52.227-03 Patent Indemnity (Apr 1984)
- 52.227-06 Royalty Information (Apr 1984)
- 52.227-09 Refund of Royalties (Apr 1984)
- 52.227-19 Commercial Computer Software License (Dec 2007)
- 52.225-5 Trade Agreements (Oct 2019)
- 52.232-39 Unenforceability of Unauthorized Obligations (Jun 2013)
- 52.232-40 Providing Accelerated Payments to Small Business Subcontractors (Dec 2013)
- 52.239-1 Privacy or Security Safeguards (Aug 1996)

- 252.201-7000 CONTRACTING OFFICER'S REPRESENTATIVE (DEC 1991)
- 252.203-7002 REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (SEP 2013)
- 252.203-7003 AGENCY OFFICE OF THE INSPECTOR GENERAL (AUG 2019)
- 252.203-7005 REPRESENTATION RELATING TO COMPENSATION OF FORMER DOD OFFICIALS (NOV 2011)
- 252.204-7000 DISCLOSURE OF INFORMATION (OCT 2016)
- 252.204-7002 PAYMENT FOR CONTRACT LINE OR SUBLINE ITEMS NOT SEPARATELY PRICED (APR 2020)
- 252.204-7003 CONTROL OF GOVERNMENT PERSONNEL WORK PRODUCT (APR 1992)

- 252.204-7004 LEVEL I ANTITERRORISM AWARENESS TRAINING FOR CONTRACTORS (FEB 2019)
- 252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (OCT 2016)
- 252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)
- 252.204-7016 COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES—REPRESENTATION (DEC 2019)
- 252.204-7017 PROHIBITION ON THE ACQUISITON OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES—REPRESENTATION (DEC 2019)
- 252.204-7018 PROHIBITION ON THE ACQUISITION OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES (DEC 2019)
- 252.205-7000 PROVISION OF INFORMATION TO COOPERATIVE AGREEMENT HOLDERS (DEC 1991)
- 252.211-7003 ITEM UNIQUE IDENTIFICATION AND VALUATION (MAR 2016)
- 252.215-7008 ONLY ONE OFFER (JUL 2019)
- 252.215-7013 SUPPLES AND SERVICES PROVIDED BY NONTRADITIONAL DEFENSE CONTRACTORS (JAN 2018)
- 252.227-7000 NON-ESTOPPEL (OCT 1966)
- 252.227-7015 TECHNICAL DATA—COMMERCIAL ITEMS (FEB 2014)
- 252.227-7025 LIMITATIONS ON THE USE OR DISCLOSURE OF GOVERNMENT-FURNISHED
- 252.227-7037 VALIDATION OF RESTRICTIVE MARKINGS ON TECHNICAL DATA (SEP 2016)
- 252.232-7007 LIMITATION OF GOVERNMENT S OBLIGATION (APR 2014)
- 252.232-7010 LEVIES ON CONTRACT PAYMENTS (DEC 2006)
- 252.239-7000 PROTECTION AGAINST COMPROMISING EMANATIONS (OCT 2019)
- 252.239-7001 INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION (JAN 2008)
- 252.239-7009 REPRESENTATION OF USE OF CLOUD COMPUTING (SEP 2015)
- 252.239-7010 CLOUD COMPUTING SERVICES (OCT 2016)
- 252.243-7001 PRICING OF CONTRACT MODIFICATIONS (DEC 1991)
- 252.243-7002 REQUESTS FOR EQUITABLE ADJUSTMENT (DEC 2012)
- 252.244-7000 SUBCONTRACTS FOR COMMERCIAL ITEMS AND COMMERCIAL COMPONENTS (DOD CONTRACTS) (JUN 2013)
- 252.246-7003 NOTIFICATION OF POTENTIAL SAFETY ISSUES (JUN 2013)
- 252.246-7005 NOTICE OF WARRANTY TRACKING OF SERIALIZED ITEMS (MAR 2016)
- 252.246-7006 WARRANTY TRACKING OF SERIALIZED ITEMS (MAR 2016)
- 252.247-7022 REPRESENTATION OF EXTENT OF TRANSPORTATION BY SEA (JUN 2019)
- 252.247-7023 TRANSPORTATION OF SUPPLIES BY SEA—BASIC (FEB 2019)

- 552.216-74 Task-Order and Delivery-Order Ombudsman (Jan2017)